ABSTRACT OF THE DISCLOSURE

A method and apparatus for collecting and securely transmitting biometric data over a network contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software. The camera data is digitized and a unique code which is a function of the digitized camera data, a secret key and a transaction token is attached to the digital file. The code may identify the sensor which acquired the biometric information, a time at which the biometric information was acquired, or a time interval during which the data is considered to be valid, and a unique transaction code. The data and code are transmitted over a network to a server which authenticates that the data has not been altered by recomputing the code using its own knowledge of the secret key and transaction token needed to generate the code. If the data is authentic the server then computes a biometric template using the data. This biometric template is then compared to a previously defined biometric template to identify the user and give the user access to a secured resource. Components to generate the biometric template may be included in the imaging device. A mutual authentication system may verify that both the server and the client are authentic. The system can be used for online banking and Internet commerce transactions.